BUNDESREPUBLIK DEUTSCHLAND

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Bescheinigung

Die Siemens Aktiengesellschaft in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren und Vorrichtung zur Sicherung des Zugangs zu einem Dienst in einem Telekommunikations-Netz"

am 27. Februar 1998 beim Deutschen Patentamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patentamt vorläufig die Symbole H 04 L und H 04 M der Internationalen Patentklassifikation erhalten.

München, den 20. Oktober 1998
Der Präsident des Deutschen Patentamts
Im Auftrag

Agurks

Aktenzeichen: 198 08 523.0

198 08 523.0 vom 27.2.98

Beschreibung

Verfahren und Vorrichtung zur Sicherung des Zugangs zu einem Dienst in einem Telekommunikations-Netz

Die Erfindung betrifft ein Verfahren zum Zugang eines Dienstes in einem Telekommunikationsnetz, etwa einem privaten Netz, einem Intelligenten Netz oder einem Mobilfunk-Netz von einem beliebigen Kommunikationsendgerät aus, bei dem es notwendig ist, sich mittels Eingabe von Ziffernfolgen zu authentifizieren um Zugang zu einem gewünschten Dienst zu erlangen. Außerdem betrifft die Erfindung eine Vorrichtung in einem Telekommunikations-Netz, die es ermöglicht, eine sichere Authentifizierung eines Benutzers durchzuführen im Falle eines Dienstaufrufes.

Bei einem Intelligenten Netz IN handelt es sich um eine Architektur, die es in einem Kommunikationsnetz ermöglicht, für Teilnehmer dieses Netzes Dienste anzubieten. Diese Mehrwertdienste, wie sie auch genannt werden, bieten Netzbetreibern die Gelegenheit, sich von Konkurrenten zu differenzieren und zusätzliche Einnahmequellen zu erschließen.

Um Mehrwertdienste in einem IN anbieten zu können, benötigt der Netzbetreiber in seinem Netz mindestens einen zentralen Knoten (Service Control Point), der die Informationen gespeichert hat, die für die Durchführung der Dienste notwendig sind (Speicherung der Dienstprogramme, Weiterleitung an zuständige Netzknoten etc.). Dieser zentrale Knoten wird auch durchführende Instanz genannt.

Die Teilnehmer in einem Kommunikationsnetz können dabei interessante neue Dienste in Anspruch nehmen.
Einer der bekannteren Dienste ist das sogenannte 'Credit Card Calling'. Hierbei werden dem Anrufer die Gebühren für getätigte Anrufe über seine Kreditkarte abgerechnet. Damit kein Mißbrauch betrieben werden kann, wenn zum Beispiel die Kre-

ditkarte verloren geht, ist neben der Kreditkartennummer auch die Eingabe einer privaten Personal Identification Number (PIN) notwendig, um Zugriff auf den besagten Dienst zu erlangen.

Auch bei anderen Diensten ist so ein Zugriff-Schutz vorhanden oder denkbar, zum Beispiel bei Teilnehmern in einem Mobilen Netz, einem Privaten Netz oder einem Private Virtual Network.

In diesen ganzen Fällen wird der authentisierende Zifferncode über die Tastatur des Endgerätes eingegeben und transparent (d. h. in Klartext) über die Leitungen und Vermittlungsknoten des Kommunikationsnetzes übertragen.

Hierbei ergeben sich zwei Möglichkeiten, diese Zugangscodes auszuspionieren:

a) durch Ausspähen der PIN, etwa Beobachtung des Benutzers bei der Eingabe über die Tastatur seines Endgerätes, auch durch Videoüberwachung
b) durch Abhören der PIN bei der Übertragung zwischen Endgerät und der durchführenden Instanz.

Aufgabe der Erfindung ist es, eine Möglichkeit anzugeben, wie der Zugriff auf Dienste in einem Telekommunikations-Netz sicherer gestaltet werden kann.

Diese Aufgabe wird durch ein Verfahren gemäß Patentanspruch 1 gelöst.

Das verwendete Verfahren beschreibt folgendes Vorgehen:
die eindeutige Ziffernfolge zur Zugangssicherung wird nach der Eingabe mittels einer, dem Fachmann bekannten, Verschlüsselungsfunktion oder einer mathematischen Einwegfunktion verschlüsselt.
Bei einer Einwegfunktion handelt es sich um eine mathematische Funktion $f(x)=y$, wobei y einfach zu berechnen ist, umge-

kehrt ist die Ermittlung von x aus y dagegen sehr aufwendig und nicht notwendigerweise eindeutig.
Dabei wird ein weiterer Parameter mitverschlüsselt, der sich bei jeder erneuten Eingabe der Ziffernfolge ändert. Jeder erneute Verschlüsselungsvorgang liefert demgemäß ein neues Ergebnis.
Dieses wird dann zusammen mit dem veränderbaren Parametern, direkt per Protokoll oder in eine Ziffernfolge codiert, in Multi-Frequenz Tonwahl gegebenenfalls über Vermittlungsknoten bis zur zentralen Instanz gesendet.
Die Übertragung erfolgt dabei in der gleichen Weise wie beim bisherigen Vorgehen der Authentifizierung.

In der zentralen Instanz erfolgt dann die Auswertung der übertragenen Ziffernfolge, indem aus der bekannten Einwegfunktion, der erwarteten PIN und den mitgelieferten Parametern ebenfalls ein Ergebnis berechnet und im dem empfangenen Wert verglichen wird.

Die Realisierung dieses Authentisierungsverfahrens ist vergleichsweise einfach. Verschlüsselungsverfahren sind dem Fachmann in hinreichender Menge bekannt. Die Implementierung des Verfahrens ist nur auf Benutzerseite und bei der zentralen Instanz notwendig, der Implementierungsaufwand ist gering. Eine bereits vorhandene Datenbank kann einfach erweitert werden, um ein Feld zur Speicherung der bereits empfangenen Zugangscodes.

Der Vorteil des beschriebenen Verfahrens liegt klar im Teilnehmerschutz. Der Benutzer hat keinen größeren Aufwand als in bisherigen Verfahren, denn ein Zugangscode mußte bisher schon eingegeben werden. Es wird aber wirksam verhindert, daß ein unberechtigter Teilnehmer auf fremde Kosten telefoniert. Dieser Mißbrauch ist bislang ja möglich, da bei der Eingabe etwa der Kreditkarten-Nummer es nicht Voraussetzung ist, daß der Benutzer auch in Besitz dieser Kreditkarte ist. So konnte

durch einfaches Beobachten der eingegebenen Nummer inklusive PIN der Zugang einfach erreicht werden.
In diesem Fall verhindert zusätzlich die fehlende Kenntnis über das verwendete Verschlüsselungsverfahren die ungerechtfertigte Nutzung.

Durch das Hinzufügen eines oder mehrerer veränderbarer Parameter, wie zum Beispiel eine Angabe über den Anforderungszeitpunkt, wird der Zugangscode abhörsicher gestaltet. Ein Abhörversuch im Netz (auf der Anschlußleitung etwa) wird dadurch nutzlos, da ein wiederholt benutzter Zugangscode von vorneherein abgelehnt wird.

Die Aufgabe wird durch eine Vorrichtung gemäß Patentanspruch 9 gelöst.

Dabei wird ein Gerät zur Verschlüsselung der eingegebenen PIN benutzt. Dieses Gerät benötigt eine Eingabevorrichtung (Tastatur), ähnlich der des Kommunikationsendgerätes. In dem Gerät erfolgt eine Umrechnung der eingegebenen Ziffernfolge durch die mathematische Einweg-Funktion, zusammen mit einem veränderbaren Parameter. Das Ergebnis der Berechnung wird zusammen mit dem zweiten Parameter dann in Multi-Frequenz-Tonwahlverfahren übersetzt und an das Endgerät übertragen.
Von dort aus geschieht die Übertragung bis zur zentralen Instanz.
In der zentralen Instanz wird mit dem empfangenen Zugangscode eine Authentifizierung durchgeführt.

Ein wesentlicher Vorteil dieses Vorgehens besteht, zusätzlich zu den zuvor genannten Vorteilen, in der Möglichkeit, die Nummer bereits längere Zeit vor der tatsächlichen Benutzung einzugeben. So kann zumindest das 'Ausspionieren' durch Beobachten der Eingabe der Nummer wirksam verhindert werden.

Vorteilhafte Ausgestaltungen und Weiterbildungen sind in den Unteransprüchen angegeben.

Das erfindungsgemäße Vorgehen bietet sich bei bestimmten Arten von Telekommunikationsnetzen besonders an. Hier ist in erster Linie die Architektur des Intelligenten Netzes zu nennen, bei der z. B. der Dienst 'Credit Card Calling' bereits implementiert ist. Die für das Verfahren benötigte Infrastruktur ist bereits vorhanden. Neben den Privaten Netzen, die einen Mechanismus für Zugriffe von außen benötigen, gibt es auch das VPN, das Virtual Private Network, welches ebenfalls in IN Technik realisiert wird. Zuletzt ist das Verfahren auch in Kommunikationsnetzen für Mobilfunk denkbar, auch hier muß sich der Benutzer eines Gerätes authentifizieren.

Für die veränderbaren Parameter sind viele Möglichkeiten denkbar. Im einfachsten Fall wird jedesmal eine Zufallszahl kreiert, entsprechende Generatorfunktionen für Zufallszahlen sind dem Fachmann bekannt.
Eine weitere Möglichkeit ist eine Zeitangabe, zum Beispiel eine Einteilung in ein Zeitraster beliebiger Ausprägung. In diesem Fall kann die zentrale Instanz einerseits überprüfen, ob es sich bei dem empfangenen Zugangscode um einen aktuellen Wert handelt. Zudem ist möglicherweise die zusätzliche Übertragung des veränderbaren Parameters nicht notwendig, wenn Sender und Empfänger anderweitig zeitlich synchronisiert sind.
Eine weitere Möglichkeit ist die Erzeugung einer mathematischen Reihe, mit einer Anfangszahl n, wobei sich die Folgezahl n2 aus ihrer Vorgängerzahl n1 in verschiedener Weise ergeben kann, z. B. im Aufsummieren eines festen Wertes.

Für die Art der Verschlüsselung sind dem Fachmann zahlreiche Verfahren und Funktionen bekannt. Insbesondere in der ITU Recommendation X.509 und im RFC 1938 werden verschieden aufwendige und sichere Authentifizierungs- und Verschlüsselungsverfahren vorgestellt.

In der ITU Rec. X.509 werden insbesondere zwei Verfahren vorgestellt.

Das erste, einfachere Verfahren begnügt sich mit einem Verschlüsselungsvorgang. Die Einwegfunktion f wird auf einen oder mehrere veränderbare Parameter und die PIN, möglicherweise noch erweitert um einen, dem MFV-Sender und dem Telekommunikationsdienst bekannten String, angewendet. Das Ergebnis aus f(Parameter1, [Parameter2, ...], PIN) wird in einen Ziffernstring konvertiert und dieser dann vom MFV Sender übertragen.

Eine zweistufige Verschlüsselung ist aufwendiger zu realisieren und bedarf auch mehr Rechenleistung bei Sender und Empfänger, sie bietet jedoch auch einen wesentlich höheren Schutz.
Dabei geschieht ein erster Verschlüsselungsschritt wie bei dem oben genannten, einstufigen Verfahren. Anschließend findet ein zweiter Durchgang mit einem zweiten mathematischen Algorithmus f' (der mit der ersten Funktion f identisch sein kann) statt, das Ergebnis berechnet sich wie folgt:
f'(Parameter x1 [,Parameter x2,..], f(Parameter y1 [,Parameter y2], PIN), PIN).

Ein verallgemeinertes Verschlüsselungs-Vorgehen schreibt die mehrfache Anwendung eines oder verschiedener Algorithmen vor, jeweils mit den Eingabeparametern PIN und zusätzlichen veränderbaren Parametern.

Wenn das Ergebnis der Verschlüsselung keine numerische Ziffernfolge ist, oder das Ergebnis nicht ohne MVF-Töne übertragen werden kann (wie bei ISDN), so muß das Ergebnis vor der Übertragung noch in eine solche übersetzt werden.

Das Authentifizierungsverfahren überprüft den übertragenen Zifferncode. Dadurch wird festgestellt, ob der Teilnehmer Berechtigung hat zum Zugriff auf einen Dienst. Zusätzlich kann festgestellt werden, ob mit dem zum Dienstzugang berechtigenden Zugriffscode Mißbrauch betrieben wird.

Bei der Authentifizierung kann folgendermaßen vorgegangen werden:

- Es wird von der zentralen Instanz überprüft, ob der gesendete Zugangscode in einem vorgegebenen Zeitintervall bereits einmal empfangen wurde.
  Ist dies der Fall, so wird die Authentifizierung als nicht erfolgreich abgebrochen.
- Im anderen Fall berechnet die zentrale Instanz den zu erwartenden Zugangscode mittels der selben Einweg-Funktion und des im empfangenen Zugangscodes enthaltenen zweiten Parameters und vergleicht das Ergebnis mit dem empfangenen.
  Bei Übereinstimmung des berechneten und des empfangenen Zugangscodes ist die Authentisierung erfolgreich. Dem Teilnehmer wird der Zugang zu dem gewünschten Dienst gewährt.

Es kann vorteilhaft sein, die Verschlüsselungsvorrichtung in das Kommunikationsendgerät zu integrieren. So hat der Teilnehmer kein zweites Gerät, welches verloren gehen kann. Übertragungsfehler von der Verschlüsselungsvorrichtung zum Endgerät werden ebenfalls vermieden. Ein im Endgerät bereits vorhandener Generator für MFV-Töne kann verwendet und gegebenenfalls modifiziert werden.

Die Anwendungsmöglichkeiten dieses Verfahrens in einem Telekommunikations-Netz (insbesondere einem Intelligenten Netz, einem Privaten Netz oder einem Mobilen Netz) sind vielfältig. Vor allem der Gebührenaspekt stellt sowohl für den Diensterbringer als auch für den Netz-Teilnehmer einen wesentlichen Faktor dar.
Gerade bei Credit Card Telefonie ist ein sehr großes Risiko gegeben. Insbesondere da in dem Fall des Mißbrauchs kein Verlust der Karte bemerkt wird und erst die nächste Rechnung das Ausmaß des Schadens offenbart.
Hier kann mit vergleichsweise geringem Aufwand ein für beide Seiten sehr hoher Nutzen erzielt werden.

Im folgenden wird die Erfindung anhand von Ausführungsbeispielen erläutert. Dabei zeigen
Figur 1 die Erzeugung, Übertragung und Authentifizierung eines Einmal-Zugangscodes in einem Intelligenten Netz,
Figur 2 die Generierung des Einmal-Zugangscodes nach ITU X.509, einstufiges Verfahren, und
Figur 3 die Generierung des Einmal-Zugangscodes nach ITU X.509, zweistufiges Verfahren.

Figur 1 zeigt den Weg eines Zugangsschlüssels (PIN) vom Teilnehmer bis zu einer zentralen Instanz (SCP) in einem Intelligenten Netz.
Nach der Eingabe in eine Vorrichtung zur Verschlüsselung (MFV) wird die PIN mittels Multi-Frequenz Wähltönen an das Endgerät (KE) und von dort in das Kommunikationsnetz zur zentralen Instanz (SCP) übertragen. Auf dem Weg werden Vermittlungsstellen (SSP) passiert, über die der verschlüsselte Zugangscode derzeit transparent übertragen wird. Hierbei könnte der Zugangscode durch Abhören ausspioniert werden. Die zentralen Instanz (SCP) überprüft den Zugangscode anhand von bereits bekannten Daten, z. B. aus einer Datenbank (DB), und den mitgelieferten Daten aus dem angelieferten Ziffernstring. Nach Berechnung des zu erwarteten Zugangscodes und Vergleich mit dem erhaltenen wird eine Rückmeldung gemacht, ob der übermittelte Zugangscode korrekt und der Zugriff des Teilnehmers daher gestattet ist, oder nicht.

Figur 2 und Figur 3 zeigen schematisch die Generierung eines Zugangscodes, der über das Netz zur zentralen Instanz übertragen werden soll. Dabei ist ein symmetrischer Schlüssel benötigt (PIN), der beim Teilnehmer und bei der zentralen Instanz, die eine Authentifizierung durchführt, bekannt ist. Die PIN selber wird nicht unverschlüsselt übertragen. Zusätzlich werden hier zwei variable Parameter mit verschlüsselt, eine Zeitangabe (Zeit, Zeit') und eine Zufallszahl. Diese Komponenten ändern sich bei jedem Authentifizierungsvorgang und verhindern somit, daß ein abgehörter Einmal-Zu-

gangscode wiederverwertet werden kann. Sofern diese Komponenten nicht bei der zentralen Instanz automatisch abgeleitet werden können, müssen sie bei der Authentifizierung mit übertragen werden.

Zusätzliche Daten, wie z. B. ein beliebiger Text, können in die Bildung des Einmal-Zugangscodes mit einfließen. Diese Daten sind entweder auf beiden Seiten bekannt oder ableitbar oder werden zusätzlich übertragen.

Mit der Einweg-Funktion f (und f') wird ein verschlüsselter Zugangscode (rpPIN) erzeugt.

Literaturverzeichnis

ITU-T X.509
Information Technology - Open Systems Interconnection -
The Directory: Authentication Framework
ITU-T Recommendation X.509, 11/93

RFC 1938
Request for Comments: 1938, May 1996
A one-Time Password System
N. Haller, Bellcore, C. Metz, Kaman Sciences Corporation

Abkürzungsverzeichnis

f, f'	Mathematische Funktionen
IN	Intelligentes Netz
ITU	International Telecommuniation Union
KE	Kommunikationsendgerät
MFV	Multi-Frequenz Verfahren
PIN	Personal Identification Number
rpPIN	replayprotected PIN
SCP	Service Control Point
SSP	Service Switching Point

Patentansprüche

1. Verfahren zur Sicherung des Zugangs zu einem Dienst in einem Telekommunikations-Netz,
wobei die Zugangssicherung durch die Eingabe einer eindeutigen, nur dem Benutzer des Dienstes bekannten Ziffernfolge im Endgerät erfolgt,
und diese Ziffernfolge im Kommunikationsnetz über Vermittlungsknoten bis zu einer zentralen Instanz transparent übermittelt und dort ausgewertet wird,
dadurch gekennzeichnet, daß
die Ziffernfolge vor der Übertragung durch das Kommunikationsnetz durch mindestens einen weiteren, veränderbaren Parameter ergänzt und
mittels eines Mathematischen Algorithmus (Einwegfunktion) verschlüsselt wird, und
daß das Ergebnis dieser Funktionsberechnung mittels Multi-Frequenz Wählverfahren zur zentralen Instanz übermittelt wird und
in der zentralen Instanz eine Authentifizierung durchgeführt wird.

2. Verfahren nach Patentanspruch 1,
dadurch gekennzeichnet, daß es sich bei dem Telekommunikationsnetz um ein Intelligentes Netz handelt.

3. Verfahren nach Patentanspruch 1 oder 2,
dadurch gekennzeichnet, daß ein veränderbarer Parameter eine Zeitangabe ist.

4. Verfahren nach Patentanspruch 1 oder 2,
dadurch gekennzeichnet, daß ein veränderbarer Parameter eine Zufallszahl ist.

5. Verfahren nach Patentanspruch 1 oder 2,

dadurch gekennzeichnet, daß ein veränderbarer Parameter aus einer Folge von Zahlen genommen, beginnend mit der ganzen Zahl n, wobei sich der Nachfolger n2 einer Zahl n1 durch Berechnung ergibt.

6. Verfahren nach einem der vorherigen Patentansprüche, dadurch gekennzeichnet, daß ein einstufiges Verfahren für die Verschlüsselung verwendet wird, nach Norm ITU X.509.

7. Verfahren nach einem der vorherigen Patentansprüche, dadurch gekennzeichnet, daß ein zweistufiges Verschlüsselungsverfahren verwendet wird, nach Norm ITU X.509.

8. Verfahren nach einem der vorherigen Patentansprüche, dadurch gekennzeichnet, daß ein Verschlüsselungsverfahren verwendet wird, nach RFC 1938.

9. Verfahren nach einem der vorherigen Patentansprüche, dadurch gekennzeichnet, daß die verwendete Mathematische Funktion durch Anwendung von Hash-Funktionen ergibt.

10. Verfahren nach einem der vorherigen Patentansprüche, dadurch gekennzeichnet, daß das Ergebnis der Mathematischen Funktion vor der Übertragung noch in eine Ziffernfolge codiert werden muß.

11. Verfahren nach einem der vorherigen Patentansprüche, dadurch gekennzeichnet, daß die Authentifizierung nicht erfolgreich ist, wenn die verschlüsselte Ziffernfolge in einem vorgegebenen Zeitintervall bereits einmal gesendet wurde.

12. Verfahren nach einem der vorherigen Patentansprüche, dadurch gekennzeichnet, daß die Authentifizierung erfolgreich durchgeführt ist, wenn

a) die verschlüsselte Ziffernfolge innerhalb eines vorgegebenen Zeitintervalls zum ersten Mal übertragen wurde und

b) und die verschlüsselte Ziffernfolge mit dem von Kommunikationsdienst berechneten Ziffernfolge übereinstimmt.

13. Vorrichtung in einem Telekommunikations-Netz zur Benutzung von Diensten, die in diesem Netz angeboten werden,
mit einem Telekommunikationsendgerät (KE), welches einem Benutzer mittels einer Eingabeeinrichtung ermöglicht, einen Dienst anzuwählen und eine Ziffernfolge zur Authentifizierung einzugeben,
mit mindestens einem Vermittlungsknoten (SSP), der den Dienstaufruf und die Ziffernfolge transparent weiterleitet und
einer zentralen Instanz (SCP) in diesem Netz, die den Dienstaufruf auswertet und eine Authentifizierung des Benutzers anhand der eingegebenen Ziffernfolge durchführt,
dadurch gekennzeichnet, daß
eine Verschlüsselungs-Vorrichtung (MVF) existiert, mit einer Eingabevorrichtung für eine Ziffernfolge (PIN) und einer Recheneinrichtung zur Berechnung eines Ergebnisses aus der mathematischen Funktion (f) und der Ziffernfolge und
einer Ausgabevorrichtung zum Senden des berechneten Ergebnisses als Multi Frequenz Wählton
und die Eingabe der Authentifizierungs-Ziffernfolge in diese Vorrichtung erfolgt, dort verschlüsselt wird und das Ergebnis der Verschlüsselung im Multi-Frequenz Wählverfahren über das Endgerät in das Netz übertragen wird und
in der zentralen Instanz eine Authentifizierungsprozedur durchgeführt wird, bevor ein Zugang zu dem angewählten Dienst in dem Intelligenten Netz gestattet wird.

14. Vorrichtung nach Patentanspruch 13,
dadurch gekennzeichnet, daß es sich bei dem Telekommunikationsnetz um ein Intelligentes Netz handelt.

15. Vorrichtung nach Patentanspruch 13,
dadurch gekennzeichnet, daß es sich bei dem Telekommunikationsnetz um ein Netz für Mobil-Telefonie handelt.

16. Vorrichtung nach Patentanspruch 13,
dadurch gekennzeichnet, daß die Verschlüsselungsvorrichtung ein Bestandteil des Telekommunikationsendgerätes ist.

Zusammenfassung

Die Erfindung betrifft ein Verfahren zum Zugang eines Dienstes in einem Telekommunikationsnetz, etwa einem Intelligenten Netz, einem privaten Netz oder einem Mobilfunk-Netz von einem beliebigen Kommunikationsendgerät aus. Dabei ist es notwendig, sich mittels Eingabe von Ziffernfolgen zu authentifizieren um Zugang zu dem gewünschten Dienst zu erlangen. Außerdem betrifft die Erfindung eine Vorrichtung in einem Telekommunikations-Netz, die es ermöglicht, eine sichere Authentifizierung eines Benutzers durchzuführen im Falle eines Dienstaufrufes.

Fig. 1

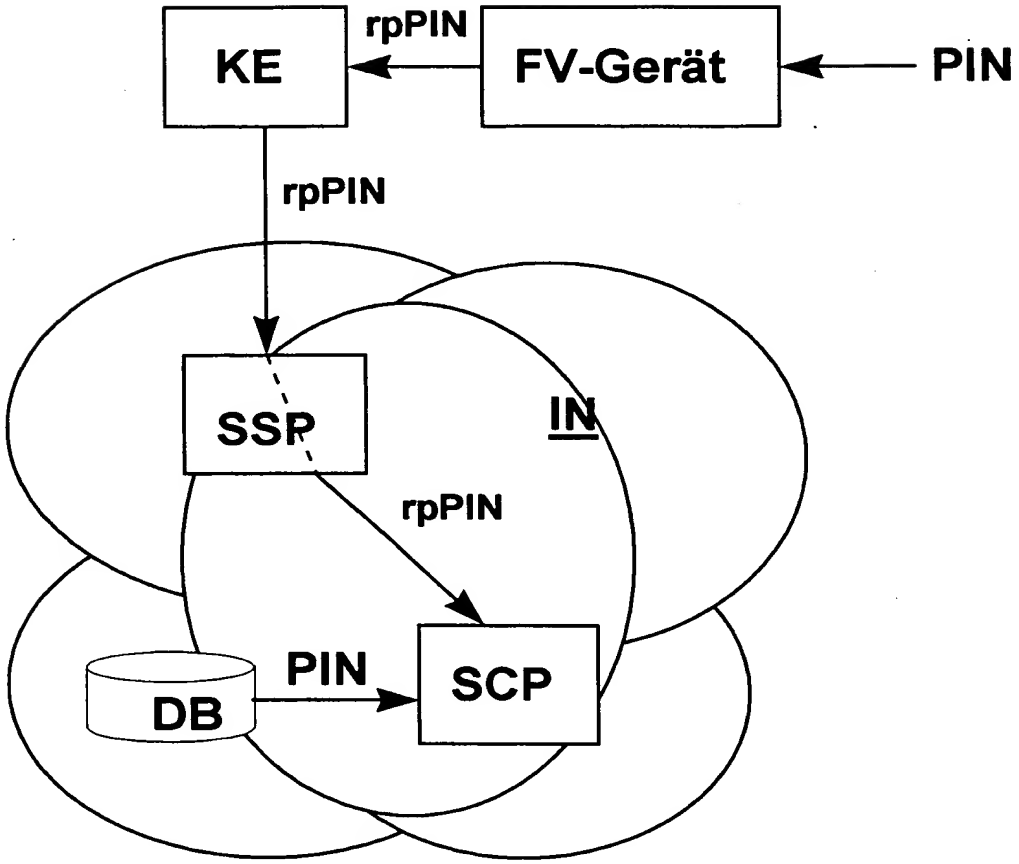

Fig. 1

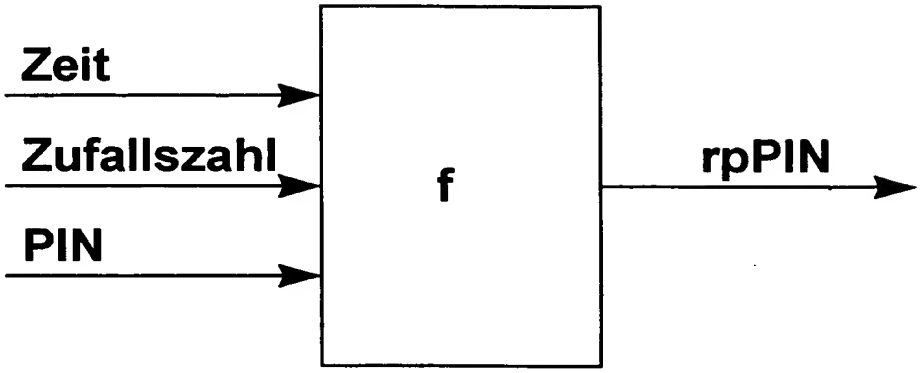

Fig. 2

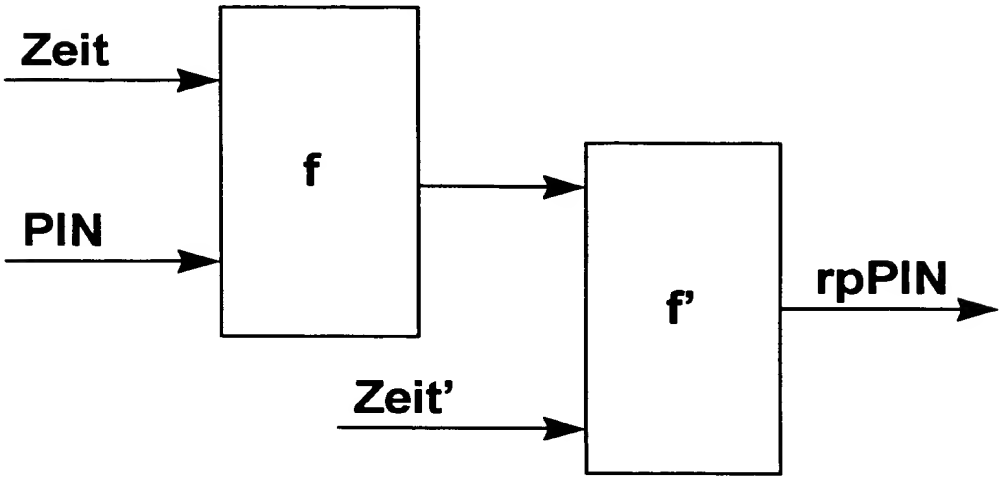

Fig. 3